

Smart Card & Identity News

Is published monthly by
Smart Card News Ltd

Head Office: Smart Card Group,
Suite 3, Anchor Springs, Duke Street,
Littlehampton, BN17 6BP

Telephone: +44 (0) 1903 734677

Fax: +44 (0) 1903 734318

Website: www.smartcard.co.uk

Email: info@smartcard.co.uk

Editorial

Managing Director – Patsy Everett

Technical Advisor – Dr David Everett

Production Team - John Owen,
Lesley Dann, Suparna Sen

Contributors to this Issue – Suparna
Sen, Carloman Grelu, Nick Senechal,
Martin Kuschewski, Tom Tainton,
Paul Johnson, Mohammad Khan

Photographic Images - Nejrion -
Dreamstime.com

Printers – Hastings Printing Company
Limited, UK

ISSN – 1755-1021

Disclaimer

Smart Card News Ltd shall not be liable for inaccuracies in its published text. We would like to make it clear that views expressed in the articles are those of the individual authors and in no way reflect our views on a particular issue.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means – including photocopying – without prior written permission from Smart Card News Ltd.

© Smart Card News Ltd

Our Comments

Dear Subscribers



Patsy Everett

Is it just me or do other people have problems with passwords? One of the side effects of the internet is that we now need a vast array of passwords to access the different sites from Amazon to PayPal and everything in between.

Now here's the thing can you have one for all these different sites?

Of course not, can't you hear the security experts screaming in your ear but actually you really don't want that many. I have a simple strategy that I don't mind sharing with you, there is the very secure password for the bank and PayPal and then there is the floppy password for all those sites that really don't matter. If you can break into my wine account (no credit card stored) and change my preferences then frankly I really don't care.

However you know what I'm about to say, real life is not like this. All these different web sites have different password strategies, no less than 8 characters, must have a number, must have a non alpha/number character, must be numeric only, it goes on and on. Well just last week I met the ultimate condition, no consecutive numbers, even just 2, up or down. Now I think my brain is starting to hurt, what nutcase decided that? In any random sequence of numbers there are bound to be consecutive numbers in one direction or the other, for my mathematical friends what are the odds in a sequence of 8 digits that at least 2 digits are consecutive? So of course you end up having to write them down, somewhere that you can lay your hands on in a hurry.

In the old days we all used to carry around those little booklet things called diaries, but now relegated to the museum we have electronic diaries in the form of mobile phones. Do you remember the Palm Pilot? Oh I felt so up to date when I first got one of those but now it's the iPhone (just wanted to drop that in, it's only the iPhone 3, you can guess who's upgraded to iPhone 4).

I wouldn't want my phone to be stolen; it stores far too much personal data. Probably all the data should be encrypted which is of course only as good as the password. But very few people seem to have their phones in encrypted mode?

Anyway all this came to mind this week when reading about the iTunes and PayPal hack with lots of people complaining about having their PayPal accounts emptied. There is not absolute clarity on exactly what has happened but the stories seem to be consistent that the hack has happened through iTunes and that somehow the fraudsters have managed to get hold of a number of iTunes account details/passwords and have then gone around doing loads of downloads funded through iTunes against PayPal. Both PayPal and iTunes have denied their systems are broken, PayPal has specifically stated that they are unaware of any account breaches on their system. iTunes have been a little more cautious suggesting that if your password has been stolen you should change it right away. Others have suggested that maybe the iTunes users were subject to some Phishing scam that resulted in the loss of their account details including the password.





Now what ever happened to 2-Factor Authentication? Just a few years ago it was on everybody's lips it was only a matter of time before we would all be carrying a smart card or token that acted to give us secure authentication into whatever sites we were registered. It's all gone quiet and yet the problems with passwords have never been more rampant. Just think about it, one smart card or token, one password for access to the smart card and hey presto you can log in securely to any web site. But more to the point the hacker without access to your smart card and password is permanently locked out, no more Phishing!

Am I missing something here?

Patsy

Contents

Regular Features

- Lead Story - India Blackberry Ban Imminent. 1
- Events Diary 3,4
- World News In Brief 7,8,11,12,14

Industry Articles

- Positive ID on a Budget: The Case for ICAO-Lite 6
- Mobile operators and financial institutions collide
 - the state of play in mobile payments 9
- Highest quality and security make the difference in e-ID projects 13
- Does AT&T's joint venture with Verizon spell the end for credit cards? . 15
- Straight to the source – securing smartcard vendors 16
- 2011: Launching Year for NFC Mobile 17

Events Diary

September 2010

- 14-15** Mobile Payment China 2010, Shanghai, China –
<http://www.mobilepaymentchina.com/mobilepayment/>
- 21-24** Smart Event '10, Sophia Antipolis, French Riviera, France -
<http://www.smart-event.eu/>
- 21-23** The Biometric Consortium Conference, Tampa, Florida, USA -
<http://www.biometrics.org/>
- 27-30** Prepaid Mobile & Mobile Payment Services 2010, Hotel Fira Palace, Barcelona, Spain
– <http://www.iir-telecoms.com/event/prepaid>, <http://www.iir-telecoms.com/event/mobilepayment/>

October 2010

- 3-5** 18th Annual ATM, Debit & Prepaid Forum, Phoenix, AZ, USA -
<http://www.paymentsource.com/conferences/atmdebit10/>
- 4-6** Cards Latin America 2010, Coral Gables, Florida –
<http://www.terrapinn.com/2010/cla/>

Source: www.smartcard.co.uk/calendar/





- 13-14 Prepaid Summit Europe 2010, Milan, Italy –
<http://www.vrl-financial-news.com/cards--payments/cards-international/events/prepaid-summit-europe-2010.aspx>
- 14 CPI Commercial Cards & Payments Summit Europe 2010, London, UK -
<http://www.commercialpaymentsinternational.com/>
- 19-21 Biometrics Exhibition and Conference 2010, Westminster, London, UK -
<http://www.biometrics2010.com/>

Source: www.smartcard.co.uk/calendar/

India Blackberry Ban Imminent Continued from page 1

Many news sources will have you believe that there will be a blanket ban on BlackBerry emails, but most likely only business users will be effected, as I will try to explain below;

There are two different set-ups for BlackBerry Email – one using BlackBerry’s Internet & Email Service (BIS) targeted towards the personal phone user and the second being the BlackBerry Enterprise Server (BES) solution for the business user.

How BIS works:

On setup, the mobile phone user provides BlackBerry (RIM) with the email addresses, connection details & credentials for each email account he/she would like to receive on their mobile phone. BlackBerry currently allows up to 10 sets of Email credentials.

BlackBerry uses the details provided to login and establish a connection on the user’s behalf to their Email server’s mailbox. BlackBerry monitors the mailboxes, and when it sees new Email, it retrieves (pulls) a copy and then pushes it to the BlackBerry handheld device over the wireless network.



Figure 1 – BlackBerry Internet Service (BIS)

Encryption is used on data travelling between each entity. The wireless network will typically use one of GSM’s family of A5 stream ciphers and if configured, BlackBerry will use a SSL session over the Internet to the E-mail server.

Although Encryption is used, it is under the control of the Network operators. BlackBerry applies compression and optimization making Email little more secure than SMS messaging. BlackBerry’s official line is: “Email messages and instant messages that are sent between the BlackBerry Internet Service and your BlackBerry device use the security features of the wireless network. Messages that are sent between your messaging server and the BlackBerry Internet Service are automatically encrypted if the server supports SSL encryption.”

How BES works:

First you must have a BlackBerry phone from the carrier on a business plan. The carrier will often lock-out the BES setup icon from a phone on a personal plan.

In this scenario the BlackBerry mobile phone user will often receive his/her phone from their company. The user is provided an activation password by the companies IT department. The next step is to launch the enterprise activation program on the BlackBerry phone and provide the activation password. The password is used to ensure the phone user is authentic and then the Enterprise Server and BlackBerry device negotiate a device transport key using following the Diffie-Hellman key agreement protocol.

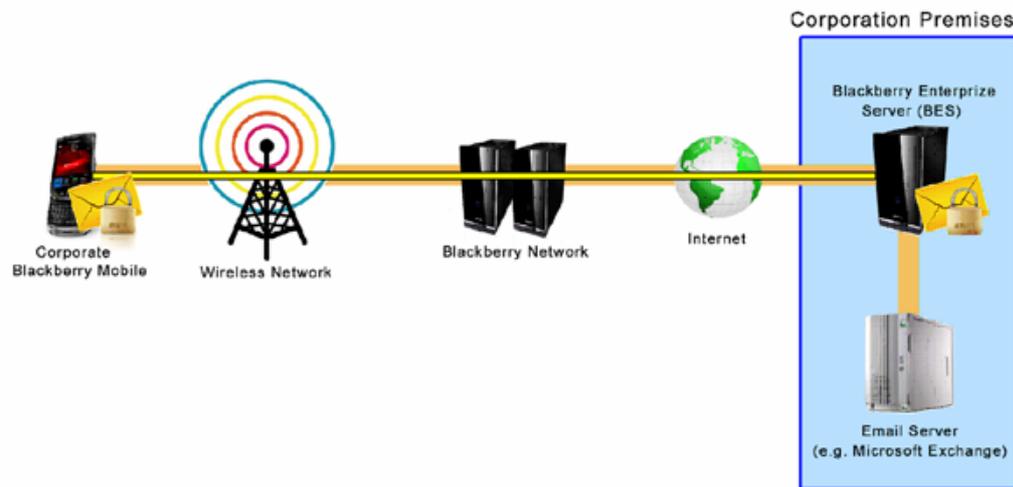


Figure 2 – BlackBerry Enterprise Server Setup (BES)

The device transport key is held on both the device and server, used to encrypt subsequent communication traffic (Application, Email & Messaging and Voice using additional BlackBerry Mobile Voice Server) using either Triple DES or AES encryption algorithms.

One final note worth mentioning regarding the BES solution is that it is possible to pay to have your BES server hosted by a 3rd party.

Telecom service providers like Airtel, Vodafone, RCom, the Tatas and the government-run BSNL and MTNL offer BlackBerry services in India. The possible ban on BlackBerry phones by the Indian Home Ministry, would see an estimated 1.1 million users having their email and chat services switched off.

Reports have suggested that the Indian government have demanded RIM on setting up a local server in its territory or to provide a master decryption key. If RIM's documentation regarding the BES solution is to be believed then there is no master key. Keys are generated uniquely per-user per-company. Also RIM's servers just route the encrypted payloads, so a local server will be of no use either.

The Indian government fears anti-national elements could misuse BlackBerry devices, as they did during the 2008 Mumbai terrorist attack, when a Pakistani-based terrorist group - Lashkar-e-Taiba, used BlackBerries with GPS and anonymous e-mail accounts, to carry on their dreadful attacks in Mumbai city killing 166 people, including Indians and foreigners. A senior Indian officer in the country's elite Black Cat commando unit (or The National Security Guard, India's counter-terrorism unit) stated, at least 5 BlackBerry mobile phones were recovered from the attack sites.

BlackBerry is considering offering metadata of an email or SMS sent through the devices like Internet Protocol address of BlackBerry Enterprise Service and PIN and International Mobile Equipment Identity of the BlackBerry mobile. However India's security agencies actually want an uninterrupted access to BlackBerry messaging services rather than receiving metadata from the BlackBerry authorities

However, the final fate of BlackBerry's (and so of its over 1 million users) encrypted email and messaging services in India will be decided in last-minute talks by end of August, ahead of an August 31 deadline. Indian telecommunication officials said that according to RIM, the only way an email could be captured is when it temporarily stores itself in a server in a decrypted form before it gets delivered. Only time will tell what kind of solution RIM comes up with that will be accepted by India.

In many countries, the debate over the BlackBerry ban has resulted in a considerable cut in the smartphone's sale. For instance in India, the sales of the smartphone have been adversely affected, and a few grey market dealers in Mumbai (the industrial city of India) have stopped ordering fresh stocks of BlackBerry models until RIM sorts out the issue with the government. Other cell phone brands like Nokia, Samsung and Apple are benefitting from the decline in the BlackBerry trade.

If the BlackBerry BES solution is banned, this may have knock-on consequences on other communication services using encryption such as Skype, WebEx and Live meeting.

By Suparna Sen, Smartcard & Identity News





Positive ID on a Budget: The Case for ICAO-Lite

By Carloman Grelu, Head of Sales, EMEA, INSIDE Contactless



Carloman Grelu

The complexity of many biometric-based identification schemes has collided head-on with the severe budget constraints faced by nations in the EU and worldwide and something needs to give. Before nations take risks on their own security by postponing plans for universal electronic ID schemes, the agencies responsible for security and citizen ID might want to take a second look at ICAO-Lite, a new derivative of the International Civil Aviation Organization standards for contactless chips developed under the ICAO 9303 suite.

ICAO-Lite derivatives do not require tossing out the e-Passport efforts undertaken in the past decade. In fact, they do not even require a change in microprocessor or reader architectures. A simple change in the way data is

partitioned within a non-volatile memory inside contactless hardware can lead to significant savings in both user hardware and overall system costs.

Why do security specialists need to think about re-inventing the wheel, so soon after the ICAO 9303 standards were adopted by more than 100 nations? In short, the chip sets that comply with full ICAO requirements are too costly and slow to be used for more mainstream e-ID applications, such as driver licenses and healthcare cards. In standard ICAO architectures, the memory in the contactless chip is fixed and sealed at issuance and cannot be altered. This means that for ID applications where data may change often, such as vehicle IDs and electronic benefit transfer cards, the standard ICAO ID can only be modified through costly hardware swaps. The first-generation chips cannot support points, counters, date flags and other kinds of data that change during the lifecycle of most ID documents.

Assuming wide use of e-ID, the numbers would favour modified memory, because 80 to 90 percent of future applications would require regular changes in data. Nevertheless, it would be silly to abandon the e-Passport architecture. Instead, a method of preserving the essence of ICAO 9303 without utilizing its entire protocol stack seems to make sense. Existing contactless microprocessors can be offered that comply with ICAO logical data structures, coding, and signing, while allowing far greater flexibility. The memory accessed by the microprocessor can be split between a fixed section that is signed with the issuer's secret key, and an open memory section for variable data, which can be modified as information about the card user changes.

Mission-Critical Security in a Recessionary World

The fact that social-benefit agencies are facing fiscal constraints in today's environment does not change the core demand for heightened security. End-to-end security domains require a detailed method for identifying all individuals, even those unlikely to travel internationally. Comprehensive identification does not just serve the interests of the issuing state or agency – it also ensures that citizens can manage rights and obligations for health care cards, voting cards, social benefits cards, and similar forms of ID for mutual advantage of individual and society. But this means that agencies need tools that are more flexible than current e-ID travel documents.

Some European Union nations have turned to a multi-application document based on full e-Passport architecture. Such an approach appears to be costly in initial implementations, and has also led to critiques from civil liberties advocates. If agencies instead were to opt for a “stripped-down”, modifiable model of ICAO 9303, component costs and supply chains could be reduced from the models used in e-Passport, even as greater flexibility was provided.

Existing contactless microprocessor architectures used in e-Passport and Near-Field Communications applications can easily be adjusted for ICAO-Lite. The only change comes in the configuration of the EEPROM (Electrically Erasable Programmable Read-Only Memory) block, to allow the partitioning of this EEPROM into public and private sectors. The issuer of the electronic ID can define how this memory is divided, so that it is up to an agency to determine the flexibility of counters, flags, and similar “rapid-change” sections of the memory. Consequently, driver license bureaus can define chips that manage fines and insurance data, and social-benefit agencies can create benefit cards that manage a small e-Purse along with user demographic statistics.





The wide use of contactless chips in the banking industry means that users of ICAO-Lite can leverage economies of scale already measured in hundreds of millions of chips shipped annually. A turn to ICAO-Lite can allow an easy migration away from systems based on proprietary encryption and protocols. Contactless microprocessors used in NFC applications outside e-Passports already comply with industry-wide RF communication and data-exchange standards. These standards depend on common and open file structures that do not require special module add-ons or software “shims” being added to existing readers.

Plenty of fringe benefits can be realized through a turn to ICAO-Lite, such as a block of memory big enough for high-resolution JPEG photographs or fingerprint images. In law-enforcement applications, the compatibility with NFC would allow the use of NFC-enabled phones for ID checks, thereby eliminating the need for card readers in many field applications. For users, extra memory space means room for special applets, such as an e-Purse or non-repudiation of transactions.

In a pre-2007 world, the move from e-Passport to ICAO-Lite would make good economic sense. In the economic environment of a post-recession international security regime, ICAO-Lite may turn into the only affordable option for many government agencies. Widespread adoption of ICAO-Lite can reduce costs of document issuance, reading of information in the field, and per-card costs for each citizen.

World News In Brief

Visa and Akbank to Launch Europe's First microSD-based Contactless M-Payments

Visa Europe, Europe's leading payment system, announced that it is launching Europe's first microSD-based mobile payment systems in Turkey with its technology partner, DeviceFidelity, and Akbank, one of Turkey's leading retail banks.

Akbank customers will be able to insert DeviceFidelity's In2Pay microSD into their handsets' memory card slots, turning them into contactless payments devices that can be used with Visa payWave terminals. The project will commence with Blackberry handsets, and will expand over time to include an array of devices from manufacturers including HTC, Samsung, LG, Nokia and Motorola.

Daon Software Selected for World's Largest Identity Program

Daon, the award-winning global provider of identity assurance software and services announced that India has joined a growing number of countries around the world to have chosen Daon's software for identity management. India will use the software in its Unique ID (UID), the world's largest identity program. The program, branded as Aadhaar, will eventually encompass 1.2 billion residents and the UID will become the single source of identity verification throughout the country.

Daon provides a centralised platform and client biometric infrastructure for a variety of uses including employee credentialing, government benefits programs, trusted identity services, border

management, National ID, airport e-gate systems and immigration control. On the India program, Daon is responsible for the fusion-based ABIS solution that incorporates finger, iris and face modalities.

eWise and VocaLink to Introduce New Online Payments Solution in UK

VocaLink, the international payments specialist, announced a partnership with eWise, the online financial management solutions provider, to introduce a new, safer and more secure online payments solution to the UK.

The eWise Online Banking ePayments (OBEP) network, unlike other alternative payment options, keeps financial institutions in the primary position of the payment chain, allowing them to protect and regain revenue being lost to alternative payment providers while leveraging existing online banking infrastructure. By utilising VocaLink's Immediate Payments platform in partnership with the eWise OBEP network, financial institutions will also benefit from a service that provides real-time consumer authentication, validation of sufficient funds and a guaranteed payment to the merchant.

SmartMetric Announces Release of Dual Band Biometric Cards

SmartMetric, Inc. announces that it has completed the research and development and successfully tested its latest prototype biometric card. The newest biometric card contains the feature of dual band radio transmission that enables both short and





long-range use, which is activated only via the owner's fingerprint.

The dual biometric card can be used in military bases, hospitals, work places, parking garages and offices. The new biometric card can work with the existing electronic security locks and readers, and hence organisations will not have to retrofit existing doors and lock hardware. SmartMetric's new biometric card comes in small size and includes robust features and superior identity protection.

Redesigned Biometric Passport Unveiled in UK

UK's Identity and Passport Service department unveiled its new ePassport with various security enhancements and new design features and security features such as hiding the security chip from view, and a personal details section that features holograms. The personal details move from the back to the second page, and a photograph of the owner now appears twice.

Chief Executive of the Identity and Passport Service Sarah Rapson said that the new 10-year passport will be issued with pages of the document containing well-known UK scenes, including the White Cliffs of Dover, the Gower Peninsula, Ben Nevis and the Giant's Causeway. The passport will be issued from October, this year. The value of the 10-year contract is £400 million, which is less than the previous contract, despite an enhanced product.

The government says the new passport will give UK citizens added protection from identity theft and fraud.

O2 and NatWest Split may Delay Launch of NFC and Mobile Payments

The break-up of the partnership between RBS-owned NatWest and Telefonica's O2 could call into question future developments in mobile payments and near field communications (NFC) in the UK suggest analysts at Datamonitor.

Gilles Ubaghs, analyst at Datamonitor said: "O2 will continue to market their O2 Money prepaid cards to new customers, for which they claim to have received over 100,000 applications for in the first few months of its launch".

However Gilles Ubaghs believes that the widely expected move into NFC and mobile-based payments will now be delayed for O2, as the banking industry is still under pressure to convince a new player to make the required outlay could prove difficult.

New Zealand and Australia Begin Fingerprint Immigration Checks

Immigration New Zealand (INZ) and Australia has begun fingerprint checks as part of a biometric programme to strengthen border security and prevent identity fraud. The programme will expand to include checks with the United Kingdom, Canada and the United States under the umbrella of the Five Country Conference (FCC), which has developed a system for securely, and with substantial privacy safeguards, matching fingerprint biometrics of persons of interest. Fingerprints of FCC citizens will not be shared.

The system will help INZ combat fraud and strengthen border security by helping identify, early in the immigration process, people with criminal histories or those using false identities. INZ has signed a Memorandum of Understanding (MOU) with the Australian Department of Immigration and Citizenship on 30 June 2010, and is now completing similar agreements with the UK, Canada and the US.

Google to Buy Virtual Currency Outfit Jambool at \$75M

Google has agreed a deal worth up to \$75 million to buy Jambool, the company behind Social Gold, a virtual currency platform used for online games and applications, according to TechCrunch.

Citing "multiple sources", the tech blog says Google will pay \$55 million for the company, with another \$15 million to \$20 million in an earn-out. The move pits Google squarely against Facebook and its Credit virtual currency.

MasterCard, Telefonica to Launch Co-Branded Credit Card Program

MasterCard Worldwide and Movistar, a subsidiary of Telefonica, a Spanish provider of payment and telecommunication services, have signed a multi-year agreement to issue and process co-branded credit cards in 11 countries across Latin America including Argentina, Colombia, Ecuador, El Salvador, Guatemala, Mexico, Nicaragua, Panama, Peru, Uruguay and Venezuela.

In addition, the agreement established between the two sides is set to provide Movistar-MasterCard cardholders with discounts at Movistar retailers and the ability to accumulate points that can be exchanged for phone equipment or additional airtime.



Mobile operators and financial institutions collide: the state of play in mobile payments

By Nick Senechal, head of product development at VocaLink



Nick Senechal

Mobile payments is one of a handful of technology advancements where adoption in poorer emerging economies is outstripping that in more developed countries. According to predictions by ABI Research, 170 million mobile subscribers worldwide will make domestic person-to-person payment transfers in 2011 – three times as many as those who will use their mobile phone to make other types of banking transaction. The reason behind this is attributed directly to the opportunity for the mobile channel to reach a huge population of previously unbanked people, particularly in the developing world.

In areas such as sub-Saharan Africa mobile phone ownership has enabled financial services, with payments in the vanguard, to be extended to people where no network of bank branches, internet connections or even fixed line telephones has ever existed. In these places the mobile operators have moved into the vacuum left by the absence of banks. This immediately removes one barrier to the adoption of mobile payments – that of bringing mobile operators and banks together. Contrastingly, consumers in economically developed countries such as the UK and US are currently very well-served by ATMs, internet banking and the branch network, resulting in a modest demand for mobile payments to date. But how will mobile payments adoption in the developed world play out into the future, and what factors will influence this change?

Many industry analysts are predicting a steady growth in mobile payments in the short-term. According to Gartner, ‘money transfer’ is forecasted to be the leading mobile application by 2012 in terms of factors such as its impact on consumers and industry players, potential revenue and estimated market penetration. Juniper Research predicts that almost half of global mobile subscribers – both developed and developing nations - will pay by mobile for physical and digital goods and services by 2014.

To reach this level of adoption in the developed world, there are a number of challenges that financial institutions and mobile operators must overcome. Foremost is the tipping point of this technology. Once one financial institution successfully rolls out mobile payments, it will inevitably become a strong point of differentiation, subject to copying by others and a service that must be maintained henceforward.

Clearly, the market is ready for the up-take of mobile payments. Ovum, predicts that by 2013, sales made through the mobile phone will reach £275 million, growing from £123 million in 2009. These figures show an appetite for mobile payments in the UK, as well as a clear opportunity for banks to capitalise on the familiarity consumers have with their phones. A number of factors in the mobile payments universe are changing and indicate that the tipping point has been reached and we will see significant mobile payments adoption in the developed world in the next few years.

Efficiencies in the existing infrastructure

The mobile phone is one of the most ubiquitous technologies in the world today. Mobile manufacturers and network operators themselves have seen great revenue potential in supporting mobile payments and as a result many handsets have already been developed to the point where they are secure and agile enough to host payments technology.

Alongside the availability of handsets that can host the required applications and payments technology, a suitable payments mechanism needs to be in place which matches the attributes of the mobile phone – convenience, reach and immediacy of experience - any mobile service brings with it the expectation that once a button is pressed the service will be delivered instantaneously. Thus a payment from a mobile phone needs to be able to make payments with minimal complexity, to any personal or business bank account and with instant transfer of funds.

Generally, mobile payments services to date have had some compromises on these elements. Firstly, they have often had a less than serviceable user interface requiring many keystrokes to operate. In order to achieve ‘instant transfer’ some Payment Service Providers (PSPs) have used a ‘closed loop’ model where each party has to hold or is obliged to set up an account with a single institution. This enables instant transfer of funds, but the payee then has the problem of extracting the funds from the chosen account, which adds a delay and often a fee. Linking to conventional payment systems such as ACH credit transfers or card systems has been





one alternative but has at best delivered an instant “promise to pay” not funds that can be drawn on instantly. While this process might be ok for some merchant payments, it is not what is required for mobile person-to-person payments.

The answer is to link to a real-time, immediate payment service between bank accounts. In the UK, there are two readily available immediate payment services: the LINK ATM scheme, used primarily to support cash withdrawals from ATMs and small value payments such as Mobile Phone Top-Ups and since 2008, the Faster Payments Service (FPS) which provides a real-time credit transfer service for values of up to £10,000. Both services are connected to the vast majority of bank accounts in the UK.

By using such services to support mobile payments means that not only will PSPs be able to make efficiencies by using an existing payment infrastructure as opposed to investing in a dedicated new infrastructure, but they will be able to deliver payments instantly to virtually any destination, delivering the full mobile payments proposition without compromise.

Meeting a pressing need

Not only are banks and operators technically ready to bring mobile payments to market, there are also significant industry drivers that are encouraging them to roll out the new service.

The declining use of the cheque means that banks are considering alternative payment methods. The UK Payments Council stated this year that cheques accounted for only two per cent of personal transactions in 2009 and that, even without intervention, the volume of personal cheques will more than halve to just 248 million in 2018, making up just 0.8 per cent of all personal payments. As a result, the industry is looking actively manage this decline and avoid any adverse impacts on the residual users of cheques. Part of this work is to ensure that, by 2014 a range of alternatives to cheques are available which are both accessible and acceptable to all users. The combination of the mobile channel with Immediate Payments offers the most flexible platform for a range of viable options that will cater for much of this demand.

But to restrict the business case to merely cheque replacement would be wrong. Mobile solutions must have a life of their own and will generate their own usage profile. Whilst budgets being allocated to innovation projects have certainly diminished, there is still an appetite in banks to use the mobile experience to re-build loyalty and increase customer engagement in the brand. With the core capability largely in place, mobile payments services are high on banks’ ‘to do’ lists as an option that requires little further investment but brings potentially large reputation and real financial gains.

Final barriers to mobile payments adoption

So, why have mobile payments yet to hit the mainstream? The answer lies in the fact that a number of key challenges are yet to be overcome before widespread roll-out can take place.

As we have seen above, customers in developed economies already benefit from a diverse range of secure services such as the ATM and internet banking; the mobile channel will need to offer something different, such as convenience, while at least matching existing channels in all other respects. Security is foremost amongst these and a person-to-person mobile payment must be at least as secure as the gold standard for personal payments - Chip and PIN.

In addition, mobile payment services may have to meet a raft of regulation such as the Office of Foreign Asset Control (OFAC) rules and data security standards equivalent to PCI-DSS. In a nutshell, all the processes associated with a payment initiated by a mobile phone will need to pass through numerous checks similar to those for payments initiated through other channels.

However, whilst these checks need to take place, they need to be streamlined to fit in with the “mobile ethos” of convenience and immediacy. One option under consideration is that customers will set up mobile credentials using their online banking channel and identify key credentials and short cuts such as an alias based on their phone number or regular payee details when making or receiving mobile payments. By taking this approach, a high level of security can be ensured and the transaction process is streamlined, as each payment can rely on a number of pre-existing security measures.

Another way in which banks can further secure mobile payments is to cap the payment value at a set amount, for example £250 per day. The LINK infrastructure is already used as a capped payment channel across the UK’s ATM network and could enable low value mobile payments too, resulting in the relative expense of the implementation of a mobile payments service being minimised by reusing existing architecture and connection points. For higher value payments, the Faster Payments infrastructure can be used. This may be presented over the same mobile channel, but may, for example incur an extra step in the process to validate the payment, given





the higher values involved. In this way, it can be seen that the dual service will ultimately be mutually beneficial as the deployment of each service strengthens the business case for the other.

Finally, a significant concern for banks is that they remain in control of their customers' payments. Again, the Faster Payments and LINK networks are controlled by their Member banks and thus offer the added control and certainty.

Collaboration is key

In order for mobile payments to progress to the next stage, the telecoms and financial services industry will need collaboratively. Standards to this effect will encourage further development, for example, the European Payments Council (EPC) has already commenced work on mobile payments and the roadmap shortlists SEPA card proximity payments, SEPA card mobile remote payments and SEPA Credit Transfer mobile remote payments as the priority.

In the first area, proximity payments the EPC is cooperating with the global mobile network operators represented by the GSMA and has published draft standards for contactless NFC-based payments (Near Field Communication) using the mobile phone. At the same time, draft standards for the provision of remote mobile payments have been developed through the MobeY Forum, which brings together banks, market infrastructures and mobile operators.

While the challenges to making mobile payments a reality still exist, it is clearly an area of significant growth for both banks and mobile operators in the years to come. Banks are increasingly aware of the need to provide innovative new services in order to generate additional sources of revenue and increase brand reputation. They see the mobile as a way of achieving these goals.

Whilst emerging economies have led the charge to date, in the developed economies such as the UK and US, there is growing market demand, mobile-friendly payments infrastructure, such as Faster Payments and LINK, a mature handset market which in turn enables higher levels of security and emerging standards; all of which make it likely that the many UK banks will have rolled out a mobile payments service within the next two years.

World News In Brief

CellTrust Prepares NFC-Provisioning APIs Using SecureSMS for Carriers and Banks

CellTrust Corporation, the world's largest provider of SecureSMS for mobile phones, announced that it is preparing patent-pending, NFC-provisioning APIs (Application Programming Interface) using SecureSMS, in anticipation of NFC technology rollout beginning in early 2011.

NFC (Near Field Communication) is a short-range wireless communication standard that bundles a contactless chip with a contactless reader inside the mobile device. With NFC technology, consumers can simply wave or tap their phone within a few inches of a reader to transfer information to their mobile phone or to complete a mobile payment or transaction.

Provisioning NFC with CellTrust's SecureSMS APIs addresses spoofing with a fully authenticated, government-grade, highly encrypted, tamper-proof process, which also enables message sizes up to 5,000 characters.

U.S. Telco's Looking For CEO

Major U.S. mobile carriers planning to launch an NFC-based payment service have been on a hiring mood and are preparing to order NFC phones, but are still looking for a CEO, sources told NFC Times.

The three mobile operators, Verizon, AT&T and T-Mobile USA, which have formed a joint venture, could ultimately sink hundreds of millions of dollars into the NFC-based services if they roll them out nationally, said sources. One source, citing a projection from one of the carriers, put the total investment at potentially more than \$1 billion.

At present, the telcos and their reported partners, Discover Financial Services and the U.S. arm of big British bank Barclays, are preparing for pre-commercial launches in three to four cities, expected during the second half of next year. The parties are declining to comment on their planned m-payment scheme, which would compete with Visa Inc. and MasterCard Worldwide.





USA Technologies Shipped Over 15,000 ePort Cashless Payment Terminals

USA Technologies, Inc. announced that over 20,000 ePort cashless payment terminals have been shipped or verbally committed to by customers under the JumpStart program.

JumpStart was originally launched in January 2010 to help vending operators and bottlers acquire the ePort EDGE cashless terminal at no cost, paying only a low monthly service fee, and avoiding the need to make a major upfront capital investment. The ePort EDGE, which accepts swipe cards only, is the only one-piece cashless reader and controller combo on the vending market, with PCI Level One compliant security.

The program was recently expanded to include the company's top-of-the-line ePort G8 terminal, which accepts contactless cards in addition to traditional magnetic swipe cards as well as the Get One/Buy One (GoBo) option, which enables a customer to get an ePort under a rental agreement if they commit to buying one by December 31, 2010.

Tyfone to Speak in First Forum on Alternative NFC Mobile Payment Solutions

Tyfone, the leaders and pioneers in NFC enabled Memory Cards for mobile financial services announced that their Managing Director, APAC, Prabhakar Tadepalli, will be presenting on the evolution and vision for mobile contactless payments. Tadepalli will address the current mindset in the industry and how alternative solutions are helping nourish the ecosystem to go beyond trials and for consumer deployments in 2011. Tyfone will be presenting its unique solution at the first forum on alternative NFC mobile payment solutions to be held in Taiwan on September 8-9, 2010.

The two-day forum on "Alternative NFC Mobile Payment Solutions & Bridging Gaps in the Ecosystem" is organised by the Asia Pacific Smart Card Association (APSCA), endorsed by the NFC Forum and supported by the Committee of Communications Industry Development of the Ministry of Economic Affairs of Taiwan.

TfL Gave Fresh Oyster Smartcards Contract to Cubic

New, more convenient ways to pay public transport fares are set to be developed for London's bus, rail, tube and river boat network. With the

commencement of its new three-year contract to supply all ticketing services to Transport for London (TfL). Cubic Transportation has been assigned the task of supplementing the current Oyster smartcard.

The new contract covers provision of revenue services, ticketing, information, gates and fare collection. It replaces the contract previously held by the Transys consortium in which Cubic was one of the lead partners. In 2008, TfL announced that it would be ending the contract five years early in 2010. The new arrangements will save it £10m per year.

BlockMaster's SafeStick USB Device Receives CESG Certification

Secure USB provider BlockMaster has announced that its SafeStick device has received a CESG claims test mark (CCTM) certification. Accrediting it to be the only favoured USB supplier for buyers within the public sector, Anders Pettersson, CSO at BlockMaster, claimed that it brings high attraction to the brand and the product to customers even from outside the UK. This accreditation builds on BlockMaster's existing strength within the public sector after it announced several public sector contracts with NHS Practices to supply 180,000 SafeStick devices to NHS staff last year.

RBS WorldPay Promises End-to-End Encryption for US Merchants

RBS WorldPay has struck a deal with Semtek (a leader of end-to-end encryption solutions) for the provision of end-to-end security services for its US merchants. The "multi-year" agreement will offer Semtek's Cipher Decryption service been installed on RBS WorldPay's host systems to capture transactions that have been encrypted in multiple formats.

Contactless Loyalty Scheme Gets Boost from Deal with Acquirer

Ireland's largest merchant acquirer, AIB Merchant Services, plans to roll out contactless stickers using the "loyaltyplus" service from Zapa Technology, and likewise signed a deal with the loyalty-scheme operator Zapa Technology. The company will roll out Zapa's contactless stickers more widely in Ireland and also hopes to gain a foothold in the UK.

"Loyaltyplus" service will enable consumers to tap their mobile phones or other devices to earn and redeem points for discounts and other incentives.

The joint venture has signed up retailers with a total of 120 to 150 outlets since June 2010, including a small chain in the UK.





Highest quality and security make the difference in e-ID projects

By Martin Kuschewski, Head of Business Unit eID, SMARTRAC



Martin Kuschewski

The need for reliable and trustworthy RFID-based identification documents is accepted amongst governments worldwide. From a manufacturer's perspective, supplying RFID transponders into high security applications is the accolade for any RFID-transponder producer. Supplying high security transponders into more than 40 electronic identification projects worldwide is more than this. It's a proof of highest competence and capability. The more so, as decision for a supplier follows a structured, highly competitive tender process in which every participant intends to exceed the stringent operational and technical requirements.

Electronic passports are based on smart card technology, which is widely recognised as possessing the strongest security features of any ID technology.

Applying this technology to travel documents and identity documents meets the challenge for stronger proof of identity. What decides about success or failure and what makes an RFID transponder a high security product is a combination of highly sophisticated technologies and operational processes over the entire production process of identity documents. Every single step in the manufacturing process adds security and contributes to the overall target to create a forgery-proof document that ensures reliable identification of individuals, protects the document holder's identity while at the same time enabling efficient border control processes.

One of the critical points in the manufacture of the RFID-based passport or ID-card inlay is certainly the connection between the chip and the antenna. With a lifetime of ten or fifteen years, the transponder has to sustain stresses and strains such as bending in trouser pockets, humidity and heat without failing to transmit the data over its entire lifetime. Proven interconnection technologies ensure that the data on the chip can be transmitted reliably at any time. The same consequence applies to the antenna. Securely embedded into the carrier material, the antenna will not crack or fail due to the proprietary and patented technology.

Security features of the chips and the readers are further important aspects that contribute to the overall security of e-ID documents. A product that takes concerns of travellers serious and adds another security feature to personal identification documents is the SMARTRAC eCover with Chip Activation Prevention (CAP) for electronic passports. SMARTRAC eCover with CAP ensures that personal information stored on the chip of the document can only be read from authorized parties during the identification process as it prevents the antenna from transmitting any data for as long as the passport booklet is closed. The passport holder himself has to actively open the booklet to initiate data transmission to the authorized reader. Combined with Extended Access Control (EAC) feature, passport holders and governments benefit from highest security, user convenience and efficiency.

But the all-encompassing high security concept starts at a far earlier stage of the transponder manufacturing process. Highest security means that the manufacturing facility for e-Passport and Contactless ID Card inlays itself has to comply with the most stringent security requirements. Proven by certification from an independent certification authority, the so-called "Site Certificate" ensures that the production environment for high security RFID transponders lives up to international standards.

SMARTRAC has been the first RFID inlay manufacturer who has obtained EAL 5+ security certification from the German Federal Office for Information Security (BSI) for both, the production environment and processes for the manufacture of e-ID documents as well as the initialization environment for e-ID documents for its production facility in Thailand. Evaluation Assurance Level (EAL) 5+ is currently the highest ranking international security standard applicable for the manufacture of RFID-based identity documents. The security standard is mutually recognized by commercial organizations and government bodies worldwide.

Making use of the same technological approach for both ID documents, the e-Passport and the national ID card, provides the opportunity to realize synergy effects: First of all e-ID cards with contactless chips are interoperable with the e-Passport infrastructure. Thereby, no additional infrastructure has to be built up - cost savings are the result. In addition, the identification procedure with contactless chips is secure, fast and convenient. Relying on the same technology and supplier as used for the travel documents has also advantages for the State Printing Houses and card producers: National and international ID cards are security-sensitive documents that need a certified and trusted production environment. Thus, cooperation with the same RFID inlay supplier saves an additional security checking and certification process.





Based on a network of high security production facilities in Asia, Europe and the United States, SMARTRAC continuously enhances the security level of its production facilities as well as its product offering of high security RFID inlays for e-Passports and electronic ID Cards. All of the technological developments and security measures outlined have one common target – accommodating the specific requirements of the manufacture of secure identity documents and providing customers and identity document holders equally with trusted and reliable solutions.

World News In Brief

MasterCard to Buy DataCash for £333M

MasterCard has decided to buy the European payment service provider DataCash for around £333 million. MasterCard will pay around 360 pence a share for the AIM-listed DataCash. DataCash provides a single interface for e-commerce merchants to process payments across the world and also offers fraud prevention and back-office reconciliation. MasterCard hopes the deal will enhance the MiGS gateway business currently operating in Asia Pacific, enabling merchants to gain new market reach and access to value-added services.

Visa and BofA to Test Cell Phone Payments

Bank of America Corp, the largest U.S. consumer bank, and Visa Inc, world's largest payment processor, plan to begin a test program next month that lets customers use smartphones to pay for purchases in stores.

The program, to run from September through the end of the year in the New York area, is the biggest step yet by the two companies toward creating a "digital wallet" with a host of financial capabilities built into the latest, most sophisticated mobile phones.

Intel in \$7.68bn McAfee Takeover

Under the terms of the deal, Intel will be paying \$48 per share in cash for McAfee. Through buying McAfee, a leading security technology firm, Intel intends to build security features into its microprocessors, which go into products such as laptops and phones.

The two companies said they had been working together for 18 months and the first new products would be revealed early next year. Both boards of directors have unanimously approved the deal.

NXP Selected to Secure New German National Identity Card

NXP Semiconductors N.V. announced that its SmartMX secure contactless microcontroller chip has been chosen to power the new German contactless National Identity card (Neuer Personalausweis). The German government has selected NXP as the supplier of an inlay solution containing a dedicated SmartMX chip, packaged in an ultra-thin module. Issuance of German contactless ID cards will replace the current paper-based IDs, and is about to start in November 2010. More than 60 million cards are expected to be rolled out over the next ten years.

Texan Banks Roll Out Mobile Payment Stickers

Texan banks American National and Guaranty Bond have begun offering customers 'BlingTag' contactless stickers from Bling Nation, mobile payment services, to enable cell phone payments at the point-of-sale. Each time a purchase is made using a BlingTag, the consumer receives a transaction confirmation and account balance by text message.

Since the BlingTag does not store any personal information, it offers more security than traditional plastic cards and reduces the risk of identity theft and fraud. BlingTag has won a raft of agreements with community banks across the American mid-west.

E-Kent Released Europe's First City Card

Aktif Bank, the first and only "Direct Bank" of Turkey, introduced a new banking approach by using the latest technology and considering the rapid changing customer needs. Its subsidiary company E-Kent has launched Aktif38 in Kayseri, an industrial city in Turkey. Aktif38 is a pre-paid program running on a dual interface chip, supports public transport, shopping, parking, identification and event ticketing. Individually customised card also provides special discount and bonus/loyalty points.



Does AT&T's joint venture with Verizon spell the end for credit cards?

By Tom Tainton, Smartcard & Identity News



Tom Tainton

“A mobile device is online, real-time interactivity that changes a customer relationship. A card is just dumb.” That’s the view of industry consultant Richard Crone, and a chilling indictment of the demise of debit and credit cards at the expense of contactless technology. But the world’s major pay networks, MasterCard and Visa have yet to be toppled from their ubiquitous perch. Until now, that is.

AT&T Inc. and Verizon Wireless, the USA’s largest mobile carriers are plotting a venture to oust credit and debit cards. The weapon of choice? The smartphone. Posing a new threat to Visa and Mastercard, the joint enterprise aims to develop technology that will enable American customers to buy products and services by waving their contactless phone at a reader. Although still in its primary stages, it has been reported that trials are due to begin in Atlanta and three other American cities. As part of the trials, card processor Discover will handle the payments while Barclays Bank will assist in managing the accounts.

The trials involve embedding a radio frequency identification (RFID) tag inside a phone, enabling it to be linked to a customer’s bank account. The technology allows consumers to wave their smartphone over a scanner, utilising the near field communication (NFC) capabilities stored within the device. The trial marks the carrier’s biggest effort in encouraging mobile payments in the US. Smartphones, such as Blackberry and iPhone, already lead the way in web browsing and street navigation and now it seems that they’ve set their sights on a new, gargantuan opponent. The world’s payment giants.

But with every new endeavour, there are associated challenges. For instance, starting a new payment system is difficult enough without having to get several companies to come to an agreement. In addition, it’s very expensive technology that only appeals to a small number of mobile phone subscribers. And it’s this point that has a major consequence on a key factor. The crucial middle man. The merchants. Retailers haven’t been interested in installing contactless terminals and currently only 140,000 locations have contactless readers. The reason is, of course, cash. Merchants have to spend \$200 per reader, while upgrading a smartphone with a RFID chip would cost an additional \$15. To put bluntly, consumers won’t demand mobile payments until they know that enough merchants accept them, and merchants will not implement the technology until a critical mass of consumers justifies the cost of doing so. There’s an area where the wireless carriers do hold the advantage, though. Phone companies already have access to their customer’s mobile numbers and bank account information whereas Visa and MasterCard do not.

So what would this venture, if successful, mean for Visa and MasterCard? The duo currently handles 82% of US consumer spending on credit cards that equates to around \$2.45 trillion. The dominance has helped to fuel profit growth with both companies posting annual incomes in the billions. But the AT&T and Verizon partnership could challenge the hegemony and spark a significant shift in the way in which money is transacted in the US, particularly in restaurants, shops and bars. In fact, the mobile carriers have announced aims to replace more than 1 billion plastic cards in the US alone. MasterCard and Visa will not take this lying down, however. Not by a long way. The two have been investing in their own mobile solutions, developing technology that can transform phones into payment devices with multiple card accounts. An individual’s smartphone already contains a great deal of personal information.

Developers are quick to settle any uncertainty regarding security. Several secure methods including using the smartphone’s screen as a numeric pad for accessing PIN information and using the smartphone’s sensors as a secure user-ID detection system have been suggested. But RFID technology is not impregnable. A 2006 study determined that RFID tags are susceptible to hackers and viruses such as phishing. This doesn’t seem to be a deterrent for US consumers, however. According to a Mercatus survey, almost 80% of those between 18 and 34 will use mobile financial services within five years.

It’s possible that plastic credit cards are heading towards extinction, but the final nail isn’t in the coffin just yet. Because RFID tags haven’t been extensively on American soil, it’s not yet certain that the technology will enjoy unbridled success. It’s clear that retailers, tired of complying with the hefty transaction fee demands of Visa and MasterCard, have been yearning for change, but are they prepared to put their hands in their pockets to get the ball rolling? And will consumers ignore the warning signs and trust their smartphones with sensitive data? Only time will tell.





Straight to the source – securing smartcard vendors

By Paul Johnson, director and auditing specialist, Meridian



Paul Johnson

Manufacturers of smartcards face notable compliance pressures – not only from industry bodies, but also from the companies they supply. In turn, it is the role of independent auditors to assess the logical and physical security provisions in place at the source of the smartcard supply chain, and to make recommendations as to how vendors can meet both industry and buyer imposed requirements.

Of course, almost all manufacturers are fully aware of the need for compliance, and of their audit obligations. The vast majority take their responsibilities very seriously, studiously ensuring that the annual audit is completed on time and to a high standard. But the best companies go a step further.

Compliance should not be a yearly box-ticking exercise, but an ongoing task that should be at the heart of the way the business works – not something that is only considered in the weeks leading up to a visit from an auditor. Being able to demonstrate a high level of compliance, above and beyond what is required as standard, can play a major part in securing contracts with clients, and can set a manufacturer apart from its competitors. Buyers need to feel sure that the technology they are using is safe from misuse or attack, and a comprehensive audit trail can set minds at rest.

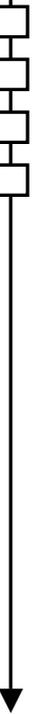
A good auditor will work with its clients throughout the year to provide consistent ongoing support on compliance issues as and when they arise, enabling them to manage risk and keep up to date with the latest developments. For example, it is not uncommon for businesses to seek to make changes to their network only a few months after qualifying to a certain standard. It is important to know what implications such changes might make to the business's ongoing certification and having experienced auditors with a strong knowledge of the industry on hand to advise can be invaluable.

Of course, the quality of advice will depend entirely on picking the right auditor for your company, and there are a number of areas to consider when appointing a company. It is paramount, for example, that you select the adviser based on the type of audit you want. This is not as strange a statement as it might first seem – an audit can be either an off-the-shelf, tick box process, or a full compliance audit.

Clearly, full compliance is the standard that companies should aim for, as it gives you a full status report on your business's position against a desired standard. Some audit companies may not employ staff with the skills to conduct a true compliance audit, which can leave their clients with an unsatisfactory result. Experienced, qualified staff will be able to carry out a thorough review that can be a part of a continuous improvement process in meeting compliance obligations – as well as being able to spot any risks that may lurk beneath the surface before they cause any serious damage.

As part of the selection process of an audit company or auditor, you should consider both the qualifications of the individual or team who will conduct the review – such as CISA or CISSP – and the company's overall standing in terms of years of experience and quality of delivery. Qualifications are all well and good, and do show that an individual has achieved the required level of understanding and has committed to abiding by a code of ethics. However, a certificate without real, tangible industry experience is worth little more than the paper it is written on.

After all, a student can leave university with a first class MSc in Information Security and ace a CISSP exam the next month. Yes, this person might have talent, and yes, they are likely to do extremely well in the future. But are they the right person to take on the responsibility of auditing a company? The short answer, unfortunately, is no. The best auditors put their qualifications into practice in a real working environment in the years following their graduation, building up the experience and knowledge they need to identify issues and establish compliance across every area of a business.





2011: Launching Year for NFC Mobile

By Mohammad Khan, President & Founder, ViVOtech, Inc



Mohammad Khan

After multiple years of industry preparation and field trials, 2011 will see Near Field Communication (NFC) mobile enter markets where contactless payment and transit solutions are most popular.

Drivers for launching NFC mobile in 2011:

- i) Add-on NFC accessories and software for existing Smartphone models
- ii) Release of multiple new NFC Smartphone models
- iii) Growing acceptance of Contactless NFC payments in specific markets
- iv) Increased clarity of business models for ecosystem players

Add-on NFC Accessories and Software for Existing Smartphone Models

An add-on NFC accessory is an NFC device that can be easily added to numerous existing Smartphone models including Blackberry, HTC, iPhone, Nokia, Samsung, and others, turning them into NFC mobile payment devices. Today, there are many NFC accessory options being used such as uSDs, SIM add-ons, sleeves/jackets, clip-ons, and Bluetooth stickers.



Enabling a Blackberry Model with NFC uSD from Device Fidelity



Enabling iPhone Model with NFC enabled with Case & uSD from Device Fidelity

ViVOtech, a leading NFC software vendor, has integrated its mobile wallet, Over the Air (OTA) provisioning software, and coupon redemption software with NFC-enabled uSD and Case accessories from Device Fidelity for multiple Blackberry models (9000, 9630, and 9700) and for the iPhone 3G and 3Gs models.

In 2011 consumers in specific markets will be able to easily upgrade their existing Smartphone models with a branded NFC mobile wallet when they buy NFC add-on accessories with supported ViVOtech mobile software and associated bank mobile payment services. In just a few minutes, they can download their payment cards from supported bank services and start using their Smartphone handsets to make payments at any Contactless enabled merchant location and start enjoying mobile coupons and offers.

Add-on NFC accessories allow leading card issuers to offer NFC payment options to their card holders without having to wait for integrated NFC handsets or the cooperation of mobile network operators (MNO).

Release of Multiple NFC Smartphone Models

Handset vendors have finally started to get serious about incorporating NFC technology into their future Smartphone models. Nokia is taking the lead again and has recently announced their plans to release some Smartphone models with NFC in 2011. Nokia, as one of three co-inventors of NFC technology along with Philips Semiconductor (now called NXP) and Sony, was also the first to provide early NFC handset models for field trials so that NFC software vendors like ViVOtech could field test complete mobile payment and marketing solutions working with industry ecosystem players.



Blackberry Device with ViVOtech Mobile Wallet Application and Device Fidelity uSD Solution





In addition to Nokia, Sagem has also announced two new models of NFC phones: Clypso targeting seniors and the Netribe an Android-based slick phone geared towards a broader user base.

Rumors that multiple handset vendors besides Nokia and Sagem are planning to release Smartphone models in 2011 are getting stronger.

NFC software is also staged for early commercial roll out in 2011. ViVOtech has made sure that its NFC payment wallet, OTA provisioning backend servers and mobile marketing/loyalty/coupon software are available for deployments at a millions of consumers' level. ViVOtech's has single NFC infrastructure software is capable of supporting all types of NFC handsets on a service provider's network, such as add-on NFC accessory enabled handsets, new embedded NFC handsets, and new SIM-based NFC (Single Wire Protocol) handsets.

Between new NFC handsets and existing Smartphone handsets with add-on NFC accessories, there will be millions of NFC handsets in circulation by end of 2011.



Sagem's Wireless Netribe Android Handset Combines NFC, Biometrics, and Good Looks

Growing Contactless NFC Payment Acceptance in Specific Markets

Thanks to the roll out of contactless payment programs under the brand names of American Express Expresspay (US only), Discover Zip (US only), MasterCard PayPass and Visa payWave, there are close to one million contactless readers deployed across the world over last five years. All of these contactless readers are backward compatible with NFC technology and are capable of branded payment transactions from NFC handsets. ViVOtech has shipped 750,000 of these one million Contactless NFC readers to 35 countries, including the United States, Canada, Australia, UK, Turkey, Taiwan, Hong Kong, Korea, Singapore, and Poland.

These specific countries are well positioned for NFC mobile payments roll out. Especially the United States, where more than 20% of Tier-1 brand name merchant locations (over 200,000 locations) are already enabled with contactless NFC readers and are ready to enjoy NFC mobile payment acceptance. An increasing number of merchants are realizing the value of NFC-enabled mobile loyalty and marketing programs and the ability to drive increased acceptance of their preferred payments through NFC mobile wallets.

Due to stronger interests in NFC mobile, ViVOtech has started to see increased deployment of contactless NFC payments in United States. ViVOtech has also started offering integrated PCI 2.1-compliant Contactless NFC PIN pad readers like the ViVOPay 8100e with EMV contact and magnetic strip card support – driving the premium price for Contactless NFC down to less than US\$50 from \$100 per unit a year ago.



New Generation of Contactless NFC PIN Pad, ViVOPay 8100e, is Making Premium Price for Contactless NFC Feature Much Lower

Increased Clarity of Business Model is Driving NFC Mobile

Another important development leading to the launch of NFC mobile in 2011 is the recognition of an effective NFC business strategy by all major ecosystem players including leading card issuers, mobile network operators (MNOs), handset vendors, and brand name merchants.

Earlier this year in Bangaluru, India, Citi in collaboration with Vodafone, MasterCard, and Nokia utilized ViVOtech NFC software to conduct Tap & Pay, one of the largest Mobile NFC Proximity Payment trials involving over 3,000 users. Edgar, Dunn and Company, an independent consultant, reported in March 2010 that the trial revealed interesting incremental business for a card issuer using NFC mobile payments and promotions as shown below.





NFC Mobile Payment & Promotion Trial **Business Results : Drives Incremental Revenue for An Issuer**

3000+ Participants Purchased NFC Phones at 200+ NFC enabled merchants in India

	Solicited Adopters	Self Adopters
Growth In Total Number of Transactions :	33%	140%
Growth in Total Purchase Value:	54%	150%
Increase in Number of Merchants Where Shopped	66%	156%

In addition to the clear business advantages for banks, both MNO's and handset vendors are recognizing that NFC handsets can be used to drive new multiple revenue opportunities by enabling merchants to drive mobile loyalty, mobile marketing and preferred payment programs. MNOs and handset vendors are also recognizing that a powerful mobile media channel can be developed through an NFC mobile infrastructure that provides a trusted channel for targeted communication to consumers on behalf of merchants, service providers and consumer product companies based on who they are, where they are, and what they are interested in. Consumers will be able to show their interest in items through interactive opt-in NFC tap technology built into their new generation of NFC handsets.

Below is an example of a consumer tapping her NFC phone on a smart poster to show her interest in receiving a coupon from a specialty store. Using ViVOtech wallet software, smart poster technology, and backend marketing campaign software, a specialty store will be able to deliver a personalized coupon based on her profile, her location and the time of day.

Merchants have started to recognize NFC mobile as a powerful media for their loyalty, merchandizing and marketing programs. Additionally, merchants have started to see the value of NFC mobile to solve the wallet share issue they have struggled with for years - plastic media used for their payment cards are only effective if consumers have them in their wallets and/or purses.

We anticipate mobile phones will become central to a consumer's shopping experience. NFC mobile will help us to find the right place to shop and the right products to buy. We will be able to simply tap our NFC phones on a shelf tag or even product tag to get more information about the product before we make a purchase. Along with the product information, there is the potential to receive an incentive if the purchase is completed within a pre-determined time frame.



Mobile phones will allow merchants to provide personalized services to consumers based on who they are and where they are. Merchants and manufacturers will be able to effectively reach out target consumers with offers and discounts through specific opt-in mobile programs. Mobile is quickly becoming the most efficient merchandizing and marketing device for at our disposal.

There is a business case for all major ecosystem players, whether they are card issuers, mobile network operators, handset vendors, or merchants.

In a year timeframe either by adding NFC technology to existing phones or with new NFC-enabled Smartphone models, NFC will start playing a major role in the lives of consumers at least in major markets where Contactless acceptance is most prevalent. The era of NFC mobile payment pilots will end and we will enter the phase of large scale commercial deployments using the experience gathered in these pilots to create innovative NFC-driven business cases based on payments, mobile loyalty, mobile merchandising, and mobile marketing.

NFC technology roll out starting in 2011 will produce major opportunities for merchants, card issuers, mobile phone operators and service providers to offer more differentiating services to their existing customers. Leading companies in this new era will be able to capitalize on their existing assets through NFC-enabled mobile infrastructure and produce new revenue streams through increased customer loyalty, additional customer base, and a new set of personalized mobile services. And the NFC mobile device will become an even more powerful tool for consumers to interact with the world around them – securely and intuitively.



Register early
and save \$500!

Mobile MONEYWORLD

LatAm 2010

Hear from:



Pablo Montesano
Global Head, New Business
Development
Telefónica S.A.



Dion Lisle
EVP, Growth Ventures
Citibank



Salvatore Pennino
Head of Cards
Deutsche Bank



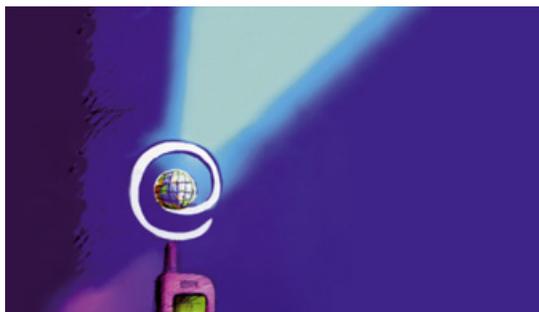
Bob Russo
General Manager
PCI Security Standards Council



Brad Garfield
Prepaid Market Manager,
Latin America
Citi Prepaid Services



Odilon Almeida
VP, Managing Director,
South America
Western Union Financial
Services International



2010 Cards Latin America



Prepaid Cards LatAm 2010



October 4 - 6, 2010, The Westin Colonnade, Coral Gables, Florida

REGISTER NOW! online www.terrappinn.com/cardslatam | **email** michael.weinberg@terrappinn.com | **phone** +1 212 379 6320 | **fax** +1 212 379 6319